USHA RAMA
COLLEGE OF ENGINEERING AND TECHNOLOGY
On NH16, Telaprolu, Near Gannavaram, Krishna Dist. – 521109
Ph.: 0866-2527558, www.usharama.edu.in
(An Autonomous Institute, Approved by AICTE, New Delhi, Permanently Affiliated to JNTUK, Kakinada)

Subject Name & Code : Cryptography and Network Security (PCIT603) Exam Name : Q1

1. In symmetric-key cryptography, the key locks and unlocks the box is [A]
A) same B) shared C) private D) public

2. The keys used in cryptography are [D]
A) secret key B) private key C) public key D) public

3. Cryptography, a word with Greek origins, means [B]
A) corrupting data B) secret writing C) open writing D) closed writing

4. A transposition cipher reorders (permutes) symbols in a [D]
A) block of packets B) block of slots C) block of signals D) block of symbols

5. Which is not an objective of network security? [D]
A) identification B) authentication C) access control D) lock

6. The process of verifying the identity of a user. [A]
A) authentication B) identification C) validation D) verification

7. Which of these is a part of network identification? [A]
A) user id B) password C) otp D) fingerprint

8. The process of transforming plain text into unreadable text. [B]
A) decryption B) encryption C) network security D) information hiding

9. A process of making the encrypted text readable again. [A]

A) decryption B) encryption C) network security D) information hiding

10. A person who enjoys learning details about computers and how to enhance their capabilities. [B]

A) cracker B) hacker C) app controller D) site controller

11. A small program that changes the way a computer operates. [D]

A) worm B) trojan C) bomb D) virus

12. An asymmetric-key (or public-key) cipher uses [B]

A) 1 key B) 2 key C) 3 key D) 4 key

13. We use cryptofraphy term to transform messages to make them secure and immune to [B]

A) change B) idle C) attacks D) defend

14. In cryptography , the original message before being transformmed , is called [B]

A) simple text B) plain text C) empty text D) filled text

15. A straight permutation cipher or a straight p-box has the same number of input as [C]

A) cipher B) frames C) outputs D) bits

16. The man-in-the-middle attack can endanger the security of the diffie-hellman if two parties are not [A]

A) authenticated B) joined C) submit D) separate

17. What is data encryption standard (DES)? [D]

A) block cipher B) stream cipher C) bit cipher D) byte cipher

18. Rail Fence Technique is an example of [B]

A) substitution B) transposition C) product cipher D) ceaser cipher

19. Public key encryption is advantageous over Symmetric key Cryptography because of [C]

A) speed B) space C) key exchange D) key length

20. The sub key length at each round of DES is [B]

A) 32 B) 56 C) 48 D) 64

21. Divide (HAPPY)26 by (SAD)26. We get quotient – [A]

A) KD B) LD C) JC D) MC

22. Dividing (11001001) by (100111) gives remainder – [D]

A) 11 B) 111 C) 101 D) 110

23. pi in terms of base 26 is [C]

A) C.DRS B) D.SQR C) D.DRS D) D.DSS

24. The time required to convert a k-bit integer to its representation in the base 10 in terms of big-O notation is [A]

A) O(log2 n) B) O(log n) C) O(log2 2n) D) O(2log n)

25. In base 26, multiplication of YES by NO gives – [C]

A) THWOE B) MPAHT C) MPJNS D) THWAE

26. Division of (131B6C3) base 16 by (lA2F) base 16 yeilds – [D]

A) 1AD B) DAD C) BAD D) 9AD

27. The estimated computations required to crack a password of 6 characters from the 26 letter alphabet is- [A]

A) 308915776 B) 11881376 C) 456976 D) 8031810176

28. What is the number of keys in conventional cryptosystem [D]

A) 2 B) 5 C) 0 D) 1

29. In Ceaser Cipher the Encrpytion algorithm is C =(P+K)mod26, the K value is [B]

A) 2 B) 3 C) 1 D) 26

30. The DES algorithm has a key length of [C]

A) 128 Bits B) 32 Bits C) 64 Bits D) 16 Bits

31. Use Caesar’s Cipher to decipher the following HQFUBSWHG WHAW [B]

A) ABANDONED LOCK B) ENCRYPTED TEXT C) ABANDONED TEXT D) ENCRYPTED LOCK

32. On Encrypting “cryptography” using Vignere Cipher System using the keyword “LUCKY” we get cipher text [A]

A) nlazeiibljji B) nlazeiibljii C) olaaeiibljki D) mlaaeiibljki

33. The Index of Coincidence for English language is approximately [C]

A) 0.068 B) 0.038 C) 0.065 D) 0.048

34. If all letters have the same chance of being chosen, the IC is approximately [D]

A) 0.065 B) 0.035 C) 0.048 D) 0.038

35. A symmetric cipher system has an IC of 0.041. What is the length of the key ‘m’? [D]

A) 1 B) 3 C) 2 D) 5

36. Caesar Cipher is an example of [B]

A) Poly alphabetic B) Mono alphabetic C) Multi alphabetic D) Bi-alphabetic

37. Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former. [B]

A) TRUE B) FALSE C) True(or)False D) one of the other

38. Which are the most frequently found letters in the English language ? [C]

A) e,a B) e,o C) e,t D) e,i

39. Choose from among the following cipher systems, from best to the worst, with respect to ease of decryption using frequency analysis. [C]

A) Plaintext, Playfair B) Playfair, Vignere C) Vignere, Playfair, Plaintext D) Plaintext

40. The Index of Coincidence is – [D]

A) 0.065 B) 0.048 C) 0.067 D) 0.044

41. Which of the following cipher is created by shuffling the letters of a word? [B]

A) substitution cipher B) transposition cipher C) mono alphabetic D) poly alphabetic

42. Which of the following is not a type of transposition cipher? [C]

A) Rail fence cipher B) Columnar transposition C) One time pad D) Route cipher

43. Which of the following is not a type of mono alphabetic cipher? [D]

A) additive cipher B) multiplicative cipher C) afffine cipher D) hill cipher

44. Route cipher falls under the category of? [C]

A) mono-alphabetic B) poly-alphabetic C) transposition D) additive

45. Which of the following ciphered text would have used transposition cipher for encryption of the plain text “SANFOUNDRY”? [D]

A) SSCMBNUMERY B) TBMGPVOESZ C) UCNHQWPFTA D) SNONRAFUDY

46. Which of the following is a type of transposition cipher? [A]

A) Rail Fence cipher B) Hill cipher C) Rotor cipher D) One time pad

47. In which of the following cipher the plain text and the ciphered text have same set of letters? [B]

A) one time pad B) columnar transposition C) playfair D) additive

48. What will be the encrypted text corresponding to plain text “SANFOUNDRY” using rail fence cipher with key value given to be 2? [A]

A) SNONRAFUDY B) SORAFUDYNN C) SNAUDNORFY D) SANFOUNDRY

49. What will be the encrypted text corresponding to plain text “SANFOUNDRY” using columnar transposition cipher with the keyword as “GAMES”? [D]

A) SNONRAFUDY B) SORAFUDYNN C) SNAUDNORFY D) ANFRSUNDOY

50. Combining transposition cipher with substitution cipher improves its strength? [A]

A) TRUE B) FALSE C) True(or)False D) none of the other

51. What does security protect? [A]

A) data B) internet systems C) hackers D) None of the mentioned

52. Who is the father of computer security? [A]

A) August Kerckhoffs B) Bob Thomas C) Robert D) Charles

53. Which of the following is defined as an attempt to steal, spy, damage or destroy computer systems, networks, or their associated information? [A]

A) Cyber attack B) Computer security C) Cryptography D) Digital hacking

54. Which of the following is a type of cyber security? [D]

A) Cloud Security B) Network Security C) Application Security D) All of the mentioned

55. What are the features of cyber security? [D]

A) Compliance B) Threat Prevention C) internal threats D) All of the mentioned

56. Which of the following is an objective of network security? [D]

A) Confidentiality B) Integrity C) Availability D) All of the mentioned

57. Which of the following is not a cybercrime? [D]

A) Denial of Service B) Man in the Middle C) Malware D) AES

58. Which of the following is a component of cyber security? [A]

A) Internet Of Things B) AI C) Database D) Attacks

59. Which of the following is a type of cyber attack? [D]

A) Phishing B) SQL Injections C) Password Attack D) All of the mentioned

60. “Cyberspace” was coined by ________ [B]

A) Richard Stallman B) William Gibson C) Andrew Tannenbaum D) Scott Fahlman

61. A _________ is a sequential segment of the memory location that is allocated for containing some data such as a character string or an array of integers. [D]

A) stack B) queue C) external storage D) buffer

62. How many types of buffer-overflow attack are there? [B]

A) 4 B) 2 C) 5 D) 3

63. _____________ is a widespread app's coding mistake made by developers which could be exploited by an attacker for gaining access [B]

A) Memory leakage B) Buffer-overrun C) Less processing power D) Inefficient programming

64. Buffer-overflow is also known as _____________ [A]

A) buffer-overrun B) buffer-leak C) memory leakage D) data overflow

65. . Buffer-overflow may remain as a bug in apps if _________ are not done fully. [C]

A) boundary hacks B) memory checks C) boundary checks D) buffer checks

66. Applications developed by programming languages like ____ and ______ have this common buffer-overflow error. [C]

A) C, Ruby B) Python, Ruby C) C, C++ D) Tcl, C#

67. Old operating systems like _______ and NT-based systems have buffer-overflow attack a common vulnerability. [D]

A) Windows 7 B) Chrome C) IOS12 D) UNIX

68. In a _attack, the extra data that holds some specific instructions in the memory for actions is projected by a cyber-criminal or penetration tester to crack the system. [C]

A) Phishing B) MiTM C) Buffer-overflow D) Clickjacking

69. ____________ attack is the exploitation of the web-session & its mechanism that is usually managed with a session token. [B]

A) Session Hacking B) Session Hijacking C) Session Cracking D) Session Compromising

70. The most commonly used session hijacking attack is the ______________ [C]

A) IP hacking B) IP spooling C) IP spoofing D) IP tracking

71. __ are required because HTTP uses a lot of diverse TCP connections, so, the web server needs a means to distinguish every user's connections. [D]

A) Internet B) Interanet C) Hijacking D) Sessions

72. Since most ___________ occur at the very beginning of the TCP session, this allows hackers to gain access to any system. [A]

A) authentications B) breaches C) integrations D) associations

73. _____________ is done only after the target user has connected to the server. [D]

A) Server hacking B) Banner grabbing C) Cracking D) Hijacking

74. In ______________ attack, the attacker doesn’t actively take over another user to perform the attack. [B]

A) phishing B) spoofing C) hijacking D) vishing

75. There are __________ types of session hijacking. [A]

A) 2 B) 3 C) 4 D) 5

76. In an ________________ attack, an attacker finds an active session & takes over that session. [C]

A) network session B) passive session C) active session D) social-networking

77. Session hijacking takes place at ___________ number of levels. [D]

A) 5 B) 4 C) 3 D) 2

78. The _____________ hijacking is implemented on the data flow of protocol shared by all web applications. [A]

A) network level B) physical level C) application level D) data level

79. Which of the following example do not comes under network level session hijacking. [C]

A) TCP/IP Hijacking B) RST Hijacking C) Domain Hijacking D) Blind Hijacking

80. In __________session hijacking, hackers gain session ID for taking control of existing session or even create a new unauthorized session. [B]

A) network level B) physical level C) application level D) data level

81. In affine block cipher systems if f(m)=Am + t, what is f(m1+m2) ? [A]

A) f(m1) + f(m2) + t B) f(m1) + f(m2) + 2t C) f(m1) + t D) f(m1) + f(m2)

82. In affine block cipher systems if f(m)=Am + t, what is f(m1+m2+m3) ? [C]

A) f(m1) + f(m2) + f(m3) + t   B) f(m1) + f(m2) + f(m3) +2t   C) f(m1) + f(m2) + f(m3)   D) 2(f(m1) + f(m2) + f(m3))

83. If the block size is ‘s’, how many affine transformations are possible ? [C]

A) 2s (2s-1)(2s-1)(2s-12)………(2s-1(s-1))   B) 2s (2s-1)(2s-2)(2s-22)………(2s-2(s-2))   C) 2ss (2s-1)(2s-2)(2s-22)………(2s-2(s-1))   D) 2s (2s-1)(2s-2)(2s-22)………(2s-2(s-3))

84. What is the number of possible keys in ceaser cipher ? [A]

A) 26   B) 126   C) 3   D) 48

85. If the key is 110100001, the output of the SP network for the plaintext: 101110001 is [B]

A) 110100011   B) 110101110   C) 10110111   D) 11111010

86. If the key is 110100001 where,If ki=0, then S_i (x)=((1 1 0 | 0 1 1 | 1 0 0))x+((1 1 1))and If ki=1, then S_i (x)=((0 1 1 | 1 0 1 | 1 0 0))x+((0 1 1))then the output of the SP network for the plaintext: 101110001 is [A]

A) 10110011   B) 111000011   C) 110110111   D) 10110110

87. Which of the following ciphers is a block cipher? [C]

A) caeser cipher   B) Playfair, Vignere   C) playfair cipher   D) none of the mentioned

88. Which of the following ciphers uses asymmetric key cryptography? [C]

A) rail fence cipher   B) DES   C) diffie hellman cipher   D) none of the mentioned

89. Block ciphers accumulate symbols in a message of a ______. [A]

A) fixed size   B) variable size   C) integration   D) All of the mentioned

90. With symmetric key algorithms, the ____ key is used for the encryption and decryption of data. [B]

A) different   B) same   C) a and b   D) none of the mentioned

91. Cipher in cryptography is – [B]

A) Encrypted message   B) Algorithm for performing encryption and decryption   C) a and b   D) Decrypted message

92. We are provided the plain text “SUN”. You need to convert the given plain text into ciphertext under the Ceasar cipher encryption technique. Which of the following options is the correct ciphertext for the given text if the key is 2 [A]

A) UWP B) NUS C) WUP D) QSL

93. Which of the following cannot be chosen as a key in the Caesar cipher? [C]

A) An integer B) An alphabet (A-Z or a-z) C) A string D) none o the mentioned

94. The Triple Data Encryption Standard (DES) is an example of a … [A]

A) Conventional cryptosystem B) Asymmetric cryptosystem C) Caesar's cryptosystem D) All of the mentioned

95. ceaser cipher is a ... Cryptosystem [A]

A) Symmetric B) Asymmetric C) Symmetric & Asymmetric both D) none of the mentioned

96. Security Goals of Cryptography are [D]

A) Confidentiality B) DATA C) Data integrityn D) All of the mentioned

97. The private key in asymmetric key cryptography is kept by [B]

A) Sender B) Receiver C) Sender and receiver D) All the connected devices to the network

98. Which one of the following algorithms is not used in asymmetric-key cryptography? [B]

A) DSA algorithm B) Electronic code book algorithm C) Diffie-Hellman algorithm D) RSA algorithm

99. Which is the cryptographic protocol that is used to protect an HTTP connection? [C]

A) Resource reservation protocol B) SCTP C) TLS D) ECN

100. ElGamal encryption system is an asymmetric key encryption algorithm. [A]

A) Public-key cryptography B) DATA C) Public-key cryptography & DATA D) none o the mentioned

101. What is the block size of plain text in SHA- 512 algorithm? [B]

A) 512 bits B) 1046 C) 2048 bits D) none o the mentioned

102. How many sub-keys in the total are used by the DES for encrypting the plain text into ciphertext? [A]

A) 16 sub- keys
B) 48 sub- keys
C) 52 sub- keys
D) Only one key and no subkeys

103. Decryption algorithms are divided into two categories based on the ______. [B]

A) Output type
B) Input type
C) Process type
D) All of the mentioned

104. Cipher block chaining or CBC is an advancement made on _____. [A]

A) Electronic Code Book
B) Decrypted code
C) System engineering
D) All of the mentioned

105. Cipher Feedback Mode is given as feedback to the ____ of encryption with some new specifications. [A]

A) Next block
B) Previous block
C) Middle block
D) All of the mentioned

106. To encrypt the plaintext, a cryptographic algorithm works in combination with a key… [A]

A) Word, number, or phrase
B) Special Symbols
C) Function Keys
D) All of the mentioned

107. A mechanism used to encrypt and decrypt data. [A]

A) Cryptography
B) DATA
C) Data flow
D) none o the mentioned

108. Modren cryptography also known as ... encryption. [A]

A) asymmetric-key
B) logical-key
C) symmetric-key
D) none o the mentioned

109. The Playfair cipher is an example of a … [A]

A) Conventional cryptosystem
B) Asymmetric cryptosystem
C) Caesar's cryptosystem
D) Public key cryptosystem

110. Using Rivest, Shamir, Adleman cryptosystem with p=7 and q=9. Encrypt M=24 to find ciphertext. The Ciphertext is: [C]

A) 42
B) 93
C) 114
D) 103

111. Which of the following is a mode of operation for the Block ciphers in cryptography? [D]

A) Electronic Code Book
B) Cipher Block Chaining (CBC)
C) Counter (CTR) mode
D) All of the mentioned

112. For which of the following should EBC (Electronic Code Book) process not be used for encryption? [C]

A) For large block sizes B) For fixed block sizes C) For small block sizes D) none o the mentioned

113. In Cipher block chaining mode, the current plaintext block is added to the ____. [A]

A) Previous ciphertext block B) Next ciphertext block C) Middle ciphertext block D) none o the mentioned

114. How many modes of operation are there in in DES and AES? [C]

A) 4 B) 3 C) 2 D) 5

115. There is a dependency on the previous ‘s’ bits in every stage in CFB mode. Here ‘s’ can range from ___ [B]

A) 8-16 bits B) 8-32 bits C) 4-16 bits D) 16 Bits

116. Which of the following modes does not implement chaining or “dependency on previous stage computations”? [A]

A) CTR, ECB B) CTR, CFB C) CFB, OFB D) ECB, OFB

117. Cryptographic hashing provides a barrier to potential _______. [A]

A) Attackers B) Sender C) Receiver D) none o the mentioned

118. Find the 8-bit word related to the polynomial x6 + x + 1 [A]

A) 1000011 B) 1000110 C) 10100110 D) 11001010

119. How many step function do Round 1 and 2 each have in S-AES? [A]

A) 4 and 3 B) either 4 C) 1 and 4 D) 3 and 4

120. The output of the previous question, on passing through “nibble substitution” gets us the output [C]

A) 3267 B) 1344 C) 64C0 D) CA37

121. How many round keys are generated in the AES algorithm? [A]

A) 11 B) 10 C) 8 D) 12

122. AES uses a ___________ bit block size and a key size of _________ bits. [D]

A) 128; 128 or 256 B) 64; 128 or 192 C) 256; 128, 192, or 256 D) 128; 128, 192, or 256

123. Which one of the following is not a cryptographic algorithm- JUPITER, Blowfish, RC6, Rijndael and Serpent? [A]

A) JUPITER B) Blowfish C) Serpent D) Rijndael

124. What is the expanded key size of AES-192? [C]

A) 44 words B) 36 words C) 52 words D) 38 words

125. The 4×4 byte matrices in the AES algorithm are called [A]

A) States B) Words C) Transitions D) Permutations

126. For the AES-128 algorithm there are __________ similar rounds and _________ round is different. [B]

A) 2 pair of 5 similar rounds ; every alternate B) 9 ; the last C) 8 ; the first and last D) 10 ; no

127. For an inputs key of size 128 bits constituting of all zeros, what is w(7) ? [A]

A) {62 63 63 63} B) {62 62 62 62} C) {00 00 00 00} D) {63 63 63 62}

128. There is no secret key in case of ____________ [A]

A) Asymmetric ciphers B) symmetric C) RSA encryption D) Alpha-numeric cryptography

129. ______ uses the concept of pseudo-random sequence. [A]

A) Stream cipher B) DES encryption C) Caesar cipher D) Block cipher

130. How many bits are there for random bits and error detection bits in the case of DES block ciphers? [B]

A) 72, 1024 B) 56, 8 C) 104, 45 D) 32, 198

131. which is most frequently used letter in english [C]

A) letter "I" B) letter"t" C) letter "e" D) letter "z"

132. Among the following given options, chose the strongest encryption technique? [D]

A) DES B) Double DES C) Triple DES D) AES

133. What is the full-form of RSA in the RSA encryption technique? [B]

A) Round Security Algorithm B) Rivest, Shamir, Adleman C) Rivest, Shamir, Azahar D) None of the mentioned

134. Codes and ciphers are different ways to _____ a message. [C]

A) Encrypt B) Decrypt C) A and B D) All of the mentioned

135. Decryption is a process to unveil the ______. [B]

A) Unsecured data B) secured C) Insecure D) None of the mentioned

136. Which of the following is /are offered by the Hash functions? [D]

A) Authentication B) Non repudiation C) Data Integrity D) All of the mentioned

137. Which of the following is not a property of Hash Function? [D]

A) Pre-Image Resistance B) Compression C) Fixed Length Output D) None of the mentioned

138.) A cryptographic hash function is an equation used to verify the ____ of data. [B]

A) Variety B) Validity C) Veracity D) None of the mentioned

139. Hash functions are used in ___ and have variable levels of complexity and difficulty. [C]

A) System approach B) Cyber safe C) Cryptography D) None of the mentioned

140. Cryptographic hashing provides a _______. [A]

A) integrity B) secrecy C) avalablity D) None of the mentioned

141. How many sub-keys in the total are used by the IDEA for encrypting the plain text into ciphertext? [C]

A) 64 sub- keys B) 48 sub- keys C) 52 sub- keys D) Only one key and no subkeys

142. Encryption algorithms are divided into two categories based on the ______. [B]

A) Output type B) data type C) Process type D) All of the mentioned

143. Cipher stream chaining or CBC is an advancement made on _____. [A]

A) Electronic Code Book B) Decrypted code C) System engineering D) All of the mentioned

144. Cipher block Mode is given as feedback to the ____ of encryption with some new specifications. [A]

A) Next block B) Previous block C) Middle block D) All of the mentioned

145. Which of the following modes of operation in DES is used for operating? [C]

A) Cipher Feedback Mode (CFB) B) Cipher Block chaining (CBC) C) Electronic code book (ECB) D) Output Feedback Modes (OFB)

146. Data encryption standard is a block cipher and encrypts data in blocks of size of _____ each. [B]

A) 16 bits B) 64 bits C) 32 bits D) All of the mentioned

147. Amongst which of the following is / are true with reference to the rounds in AES – [D]

A) Byte Substitution B) Shift Row C) row D) All of the mentioned

148. Conventional cryptography also known as ... encryption. [C]

A) asymmetric-key B) normal-key C) symmetric-key D) public key cryptosystem

149. Public key cryptography is a ... cryptosystem [B]

A) Symmetric B) asymmetric C) normal D) None of the mentioned

150. The modulus operator gives [B]

A) quotient B) reminder C) divisor D) dividend

151. In a±ne block cipher systems if f(m)=Am + t, what is f(m1+m2) ? [A]

A) f(m1) + f(m2) + t B) f(m1) + f(m2) + 2t C) f(m1) + t D) f(m1) + f(m2)

152. The attack on confidentiality is [A]

A) passive B) active C) passive & active D) no attack

153. What is the number of possible 3 x 3 affine cipher transformations ? [D]

A) 168 B) 840 C) 1024 D) 1344

154. What is the size of the key in the SDES algorithm? [D]

A) 16 bits B) 20 bits C) 12 bits D) 10 bits

155. What are the allowable values of word size in bit for RC5 algorithm? [B]

A) 16, 32 B) 16, 32, 64 C) 8, 16, 32 D) 16, 32, 48

156. The number of rounds in RC5 can range from 0 to _________ [C]

A) 127 B) 63 C) 255 D) 31

157. The standard/nominal version of the RC5-w/r/b has parameters w/r/b as [C]

A) 32/18/16 B) 16/18/16 C) 32/12/16 D) 32/16/18

158. The value of the base of natural logarithms is [B]

A) e= 2.7073 B) e= 2.7183 C) e= 3.7183 D) e= 1.7273

159. RC5 uses 2 magic constants to define their subkeys. These are [A]

A) Base of natural Logarithm and Golden ratio B) Base of natural Logarithm and Pi C) Golden Ratio and Pi D) Pi and Golden Ration

160. What does cyber security protect? [A]

A) Cyber security protects criminals B) Cyber security protects internet-connected systems C) Cyber security protects hackers D) None of the mentioned